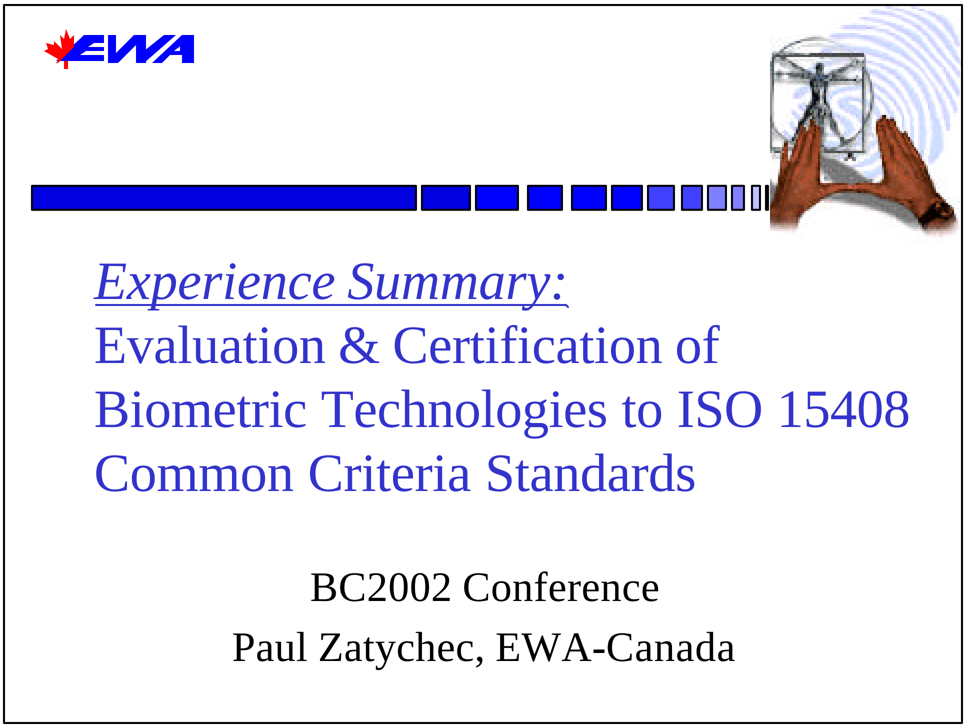
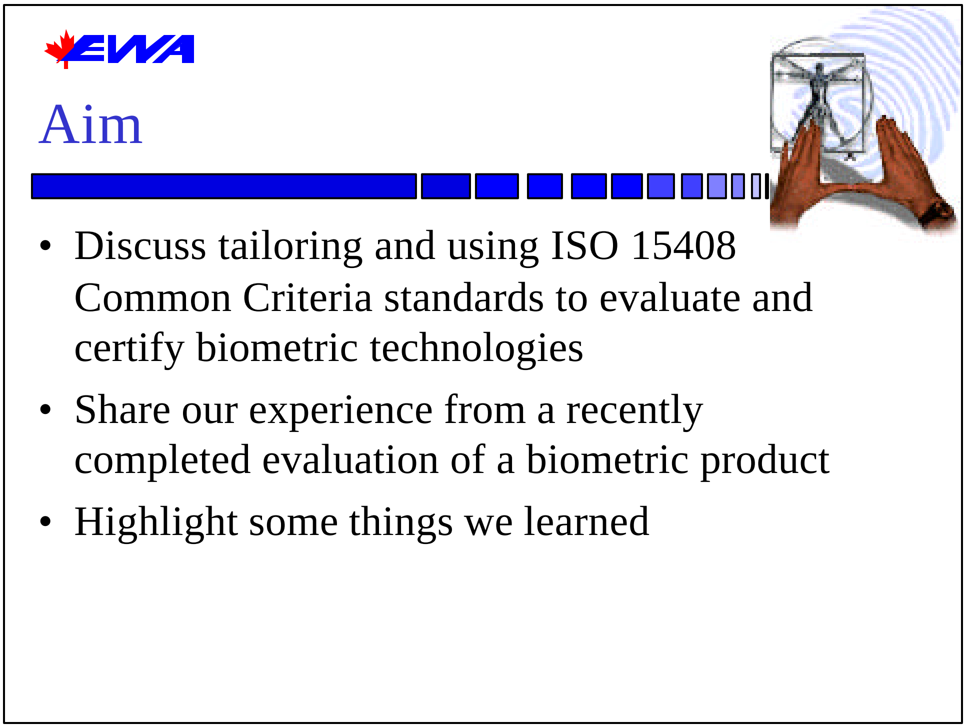


Experience Summary:

Evaluation & Certification of Biometric Technologies to ISO 15408 Common Criteria Standards

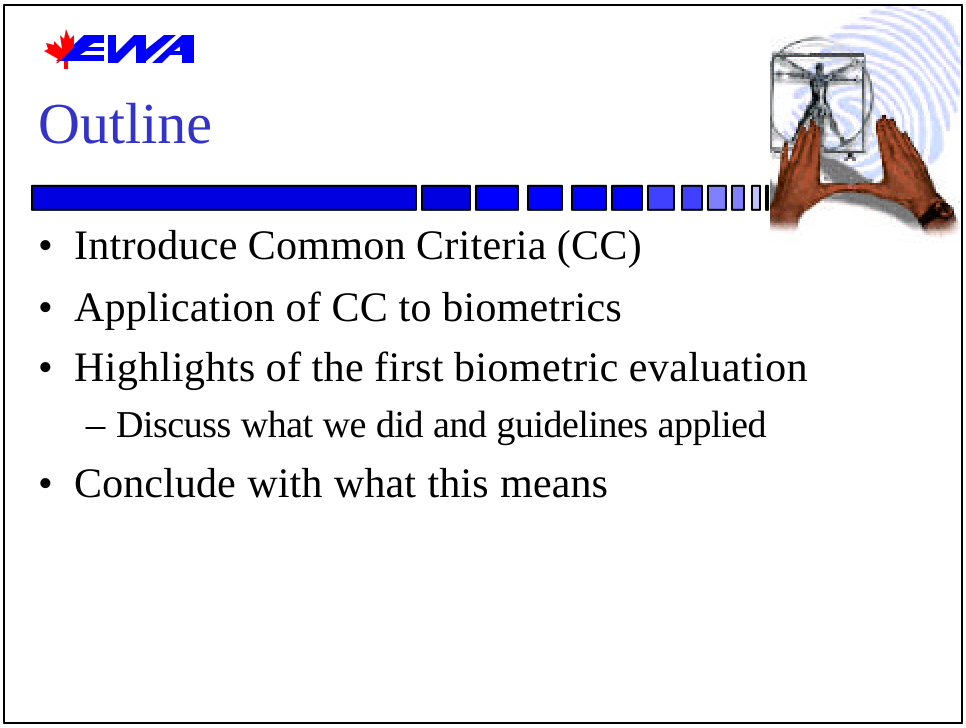
BC2002 Conference

Paul Zatychec, EWA-Canada



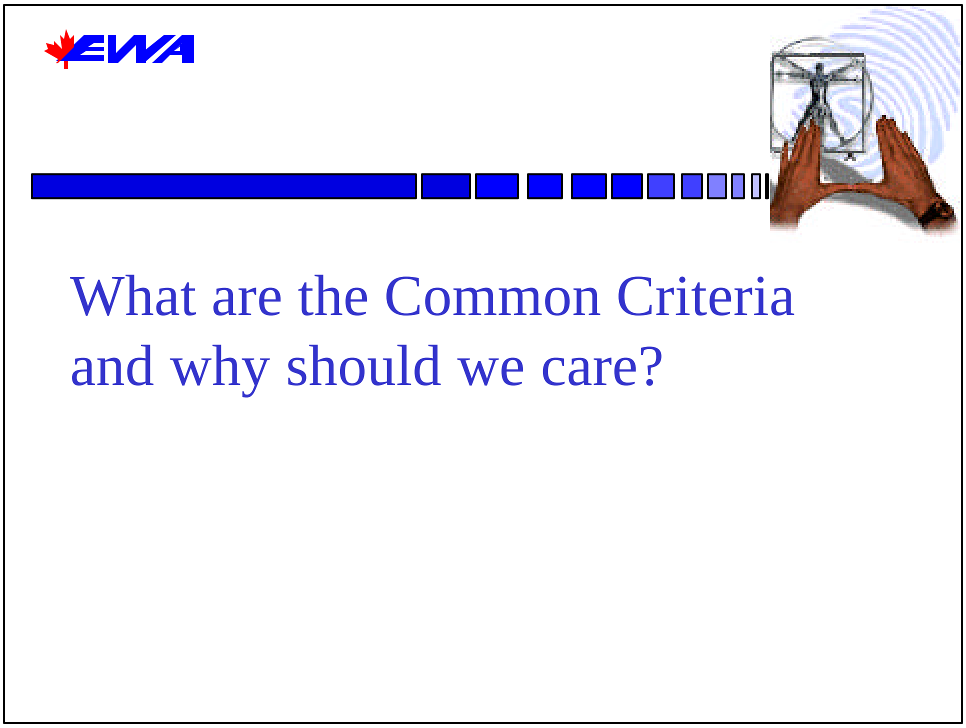
Aim

- Discuss tailoring and using ISO 15408 Common Criteria standards to evaluate and certify biometric technologies
- Share our experience from a recently completed evaluation of a biometric product
- Highlight some things we learned

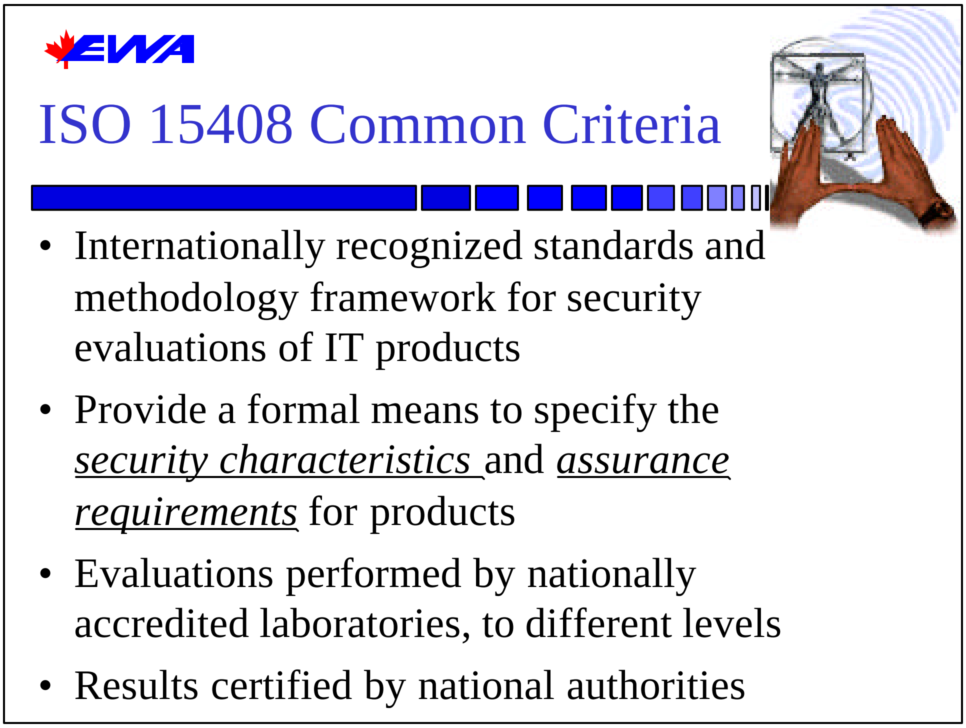


Outline

- Introduce Common Criteria (CC)
- Application of CC to biometrics
- Highlights of the first biometric evaluation
  - Discuss what we did and guidelines applied
- Conclude with what this means



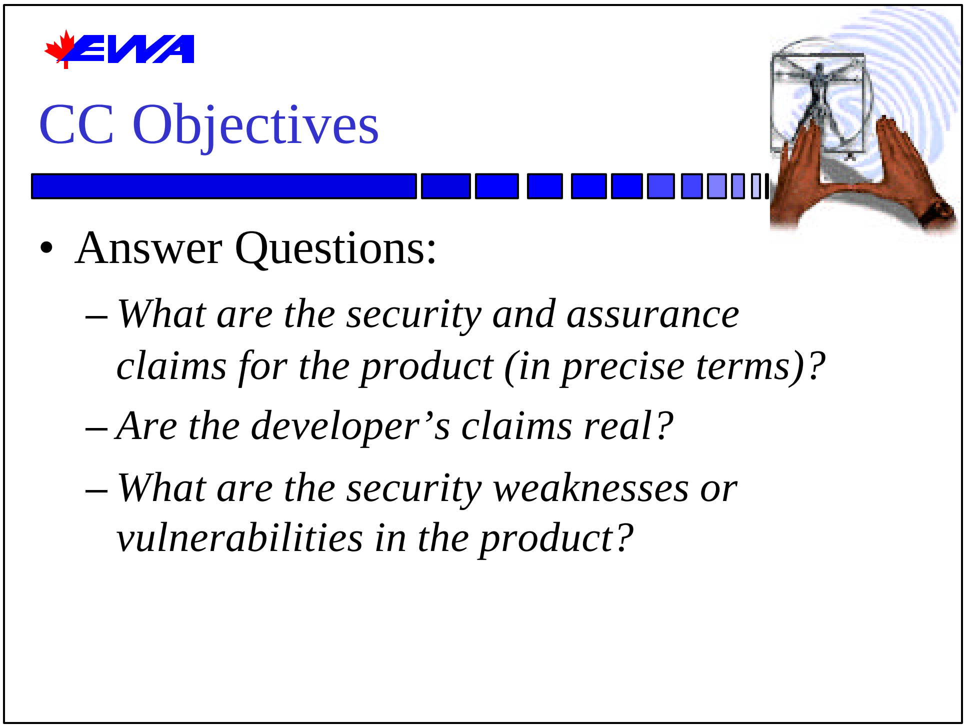
What are the Common Criteria and why should we care?



EWA

ISO 15408 Common Criteria

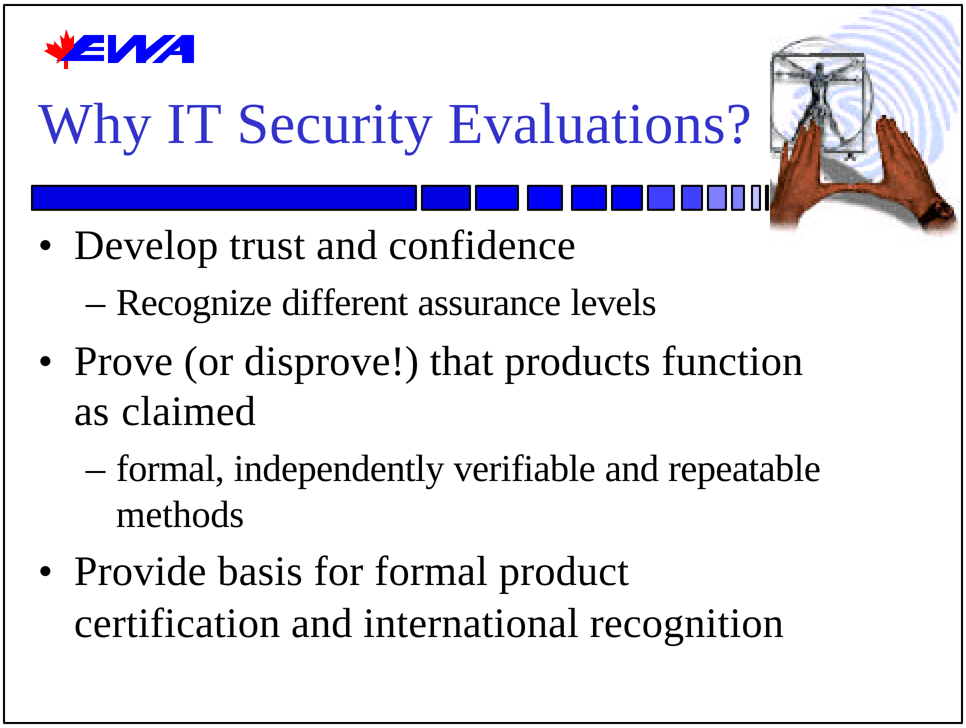
- Internationally recognized standards and methodology framework for security evaluations of IT products
- Provide a formal means to specify the *security characteristics* and *assurance requirements* for products
- Evaluations performed by nationally accredited laboratories, to different levels
- Results certified by national authorities



EWA

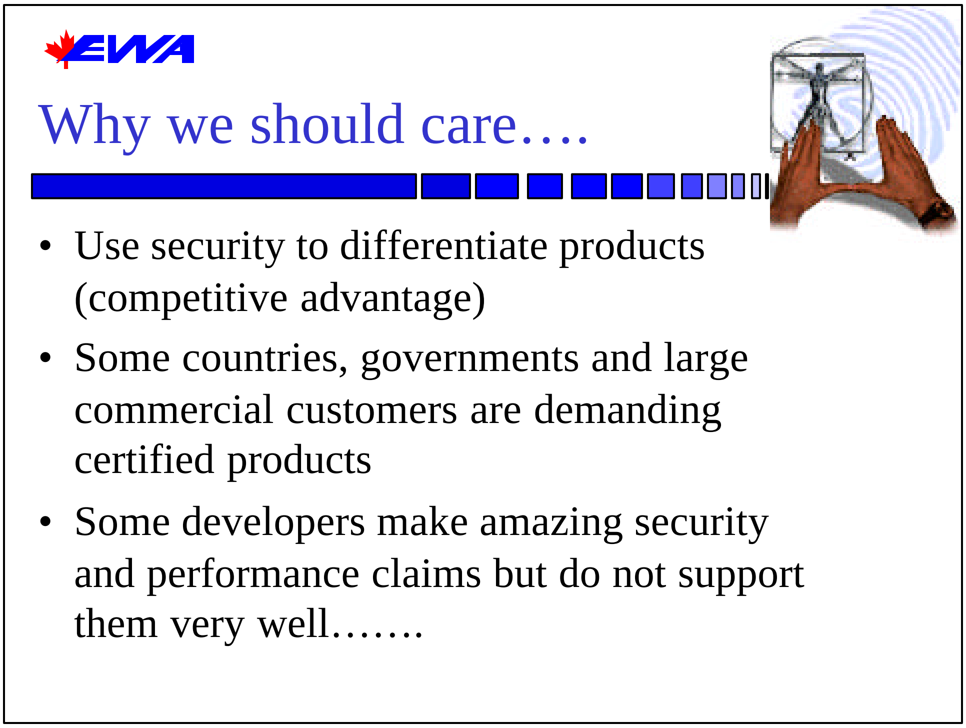
CC Objectives

- Answer Questions:
  - *What are the security and assurance claims for the product (in precise terms)?*
  - *Are the developer's claims real?*
  - *What are the security weaknesses or vulnerabilities in the product?*



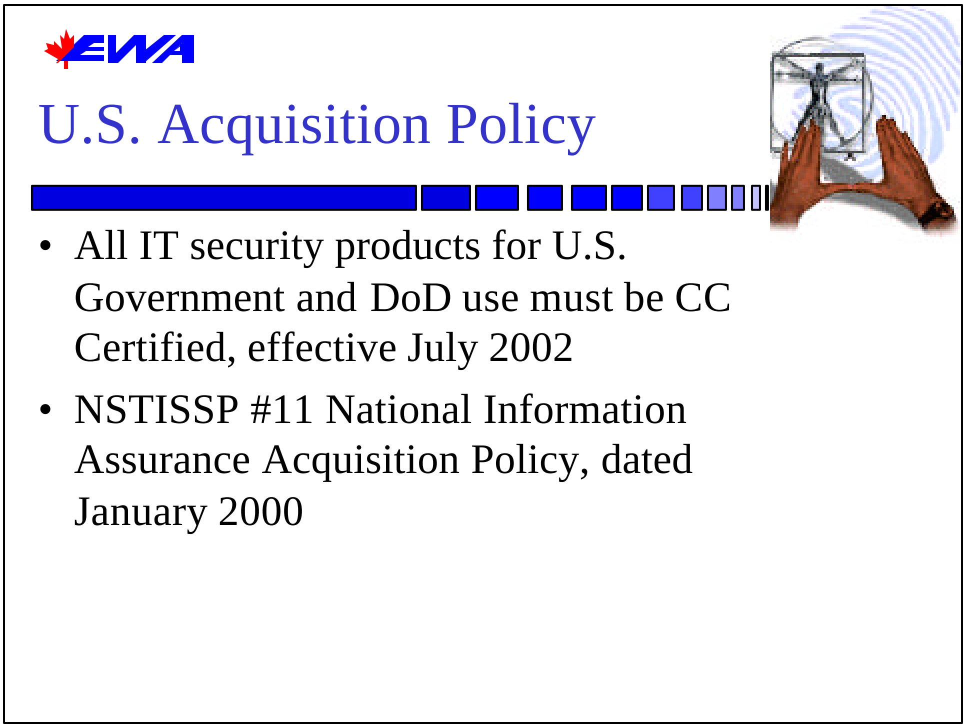
Why IT Security Evaluations?

- Develop trust and confidence
  - Recognize different assurance levels
- Prove (or disprove!) that products function as claimed
  - formal, independently verifiable and repeatable methods
- Provide basis for formal product certification and international recognition



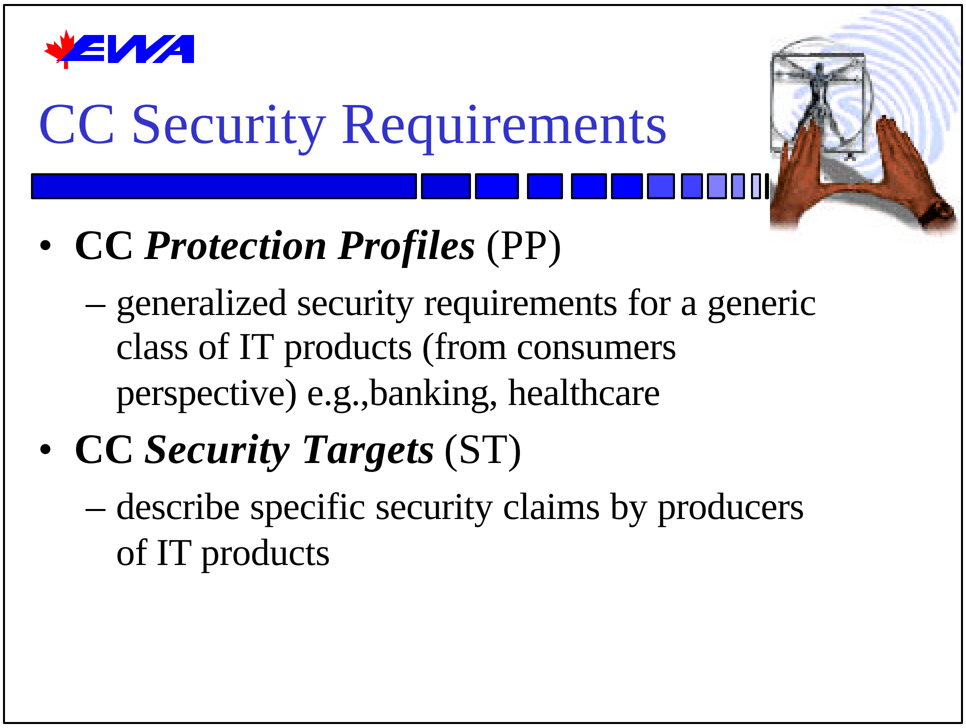
Why we should care….

- Use security to differentiate products (competitive advantage)
- Some countries, governments and large commercial customers are demanding certified products
- Some developers make amazing security and performance claims but do not support them very well…….



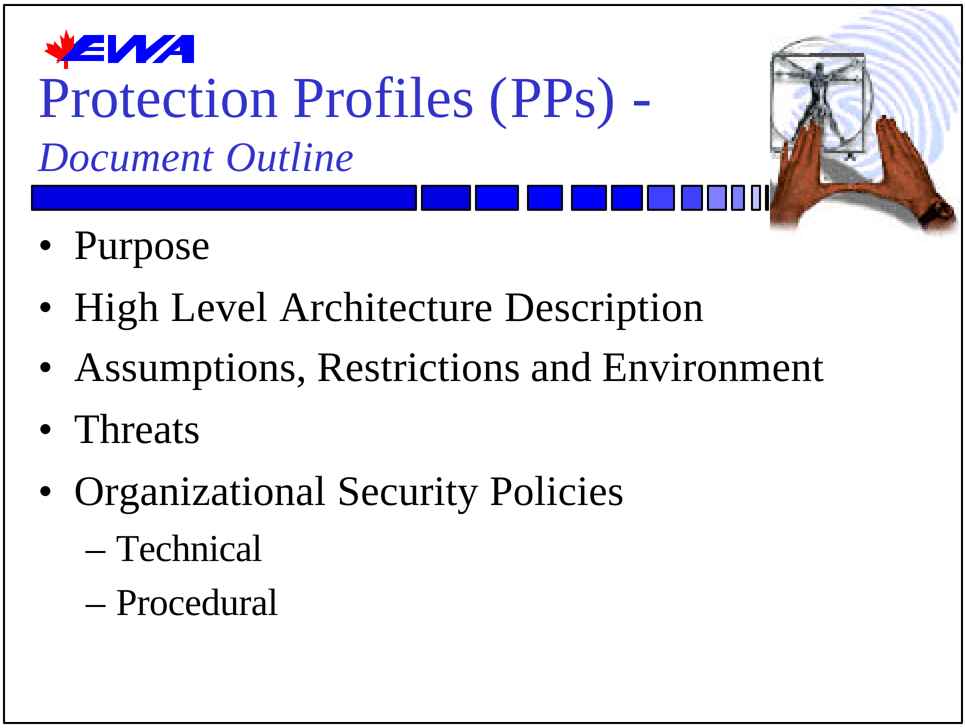
U.S. Acquisition Policy

- All IT security products for U.S. Government and DoD use must be CC Certified, effective July 2002
- NSTISSP #11 National Information Assurance Acquisition Policy, dated January 2000



CC Security Requirements

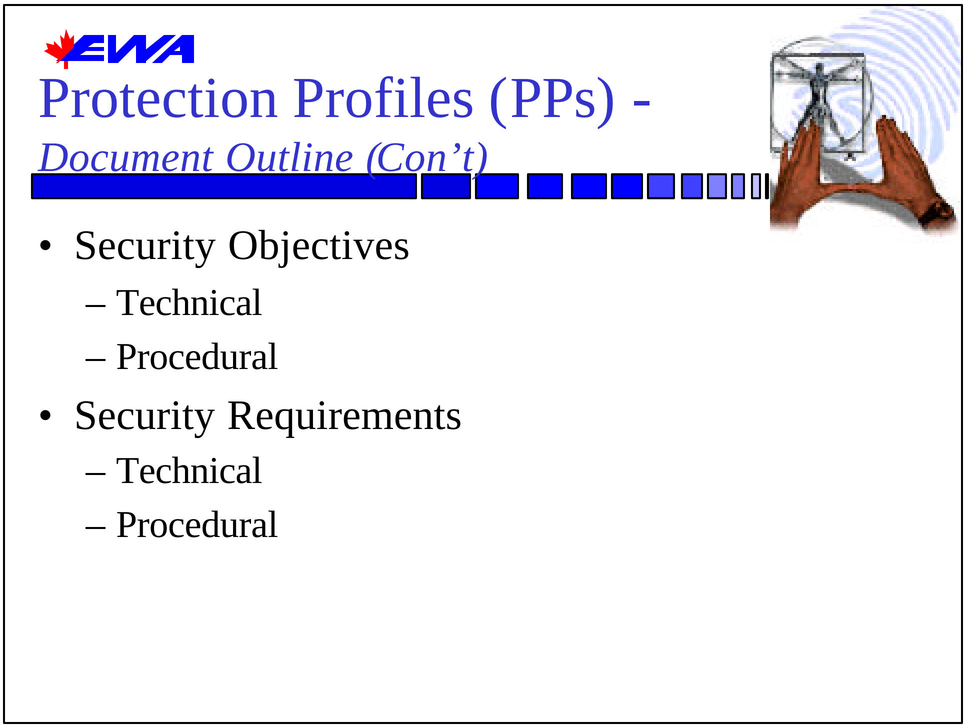
- **CC *Protection Profiles*** (PP)
  - – generalized security requirements for a generic class of IT products (from consumers perspective) e.g.,banking, healthcare
- **CC *Security Targets*** (ST)
  - – describe specific security claims by producers of IT products



Protection Profiles (PPs) -

Document Outline

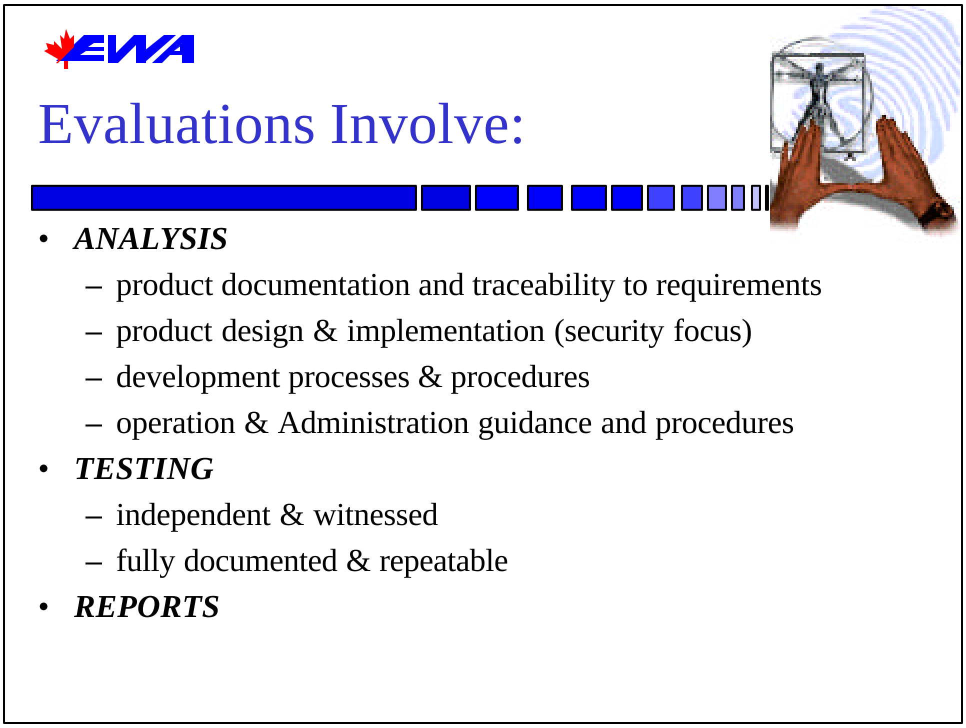
- Purpose
- High Level Architecture Description
- Assumptions, Restrictions and Environment
- Threats
- Organizational Security Policies
  - Technical
  - Procedural



Protection Profiles (PPs) -

Document Outline (Con't)

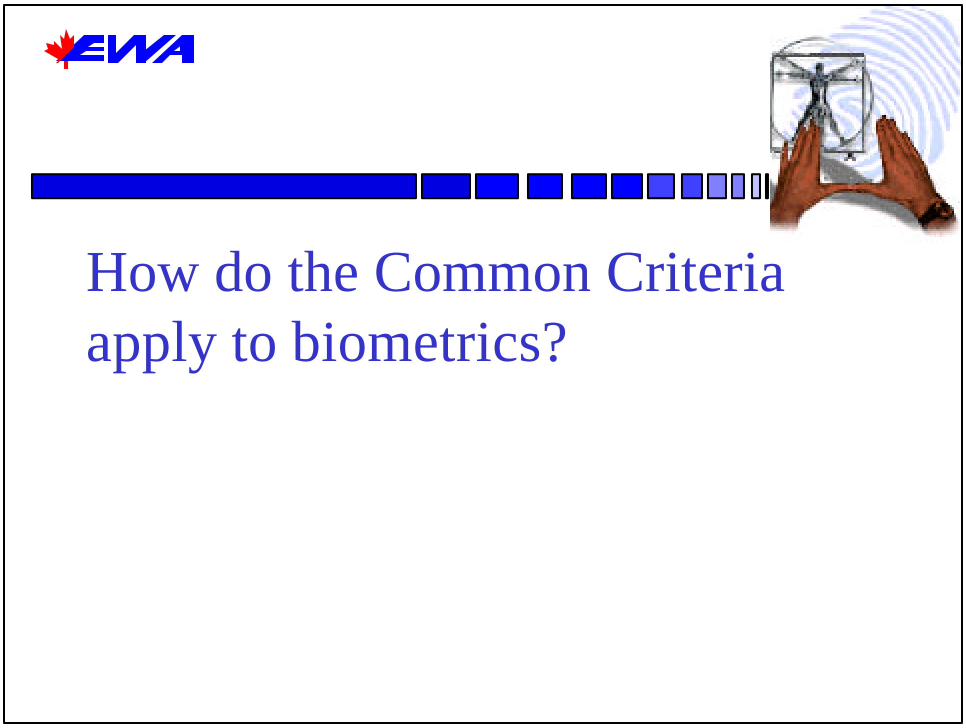
- Security Objectives
  - Technical
  - Procedural
- Security Requirements
  - Technical
  - Procedural



EWA

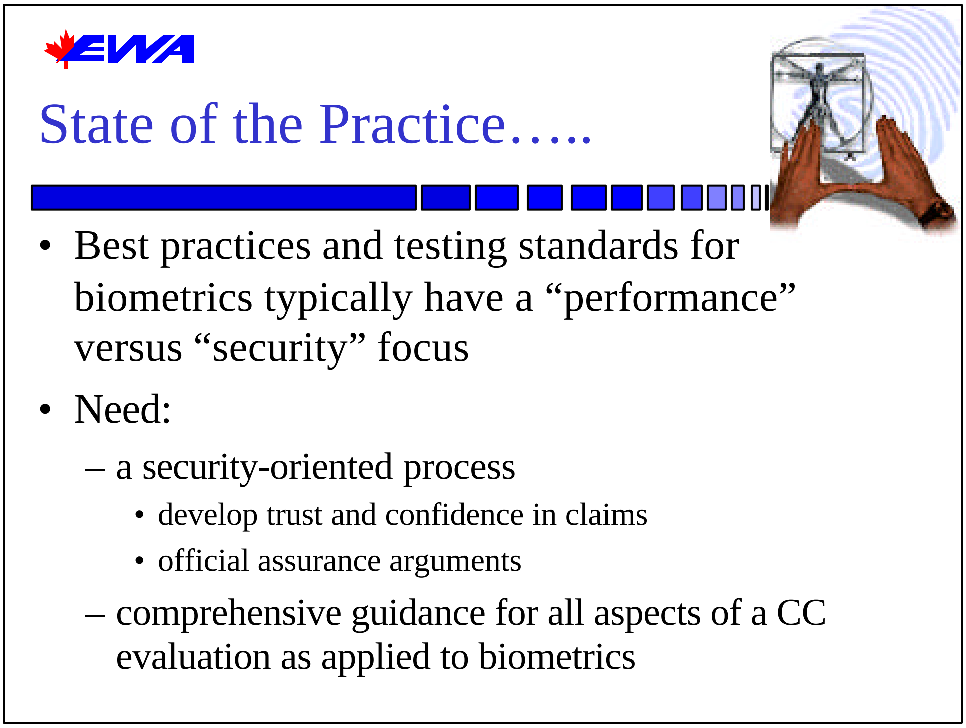
Evaluations Involve:

- ***ANALYSIS***
  - product documentation and traceability to requirements
  - product design & implementation (security focus)
  - development processes & procedures
  - operation & Administration guidance and procedures
- ***TESTING***
  - independent & witnessed
  - fully documented & repeatable
- ***REPORTS***



EWA

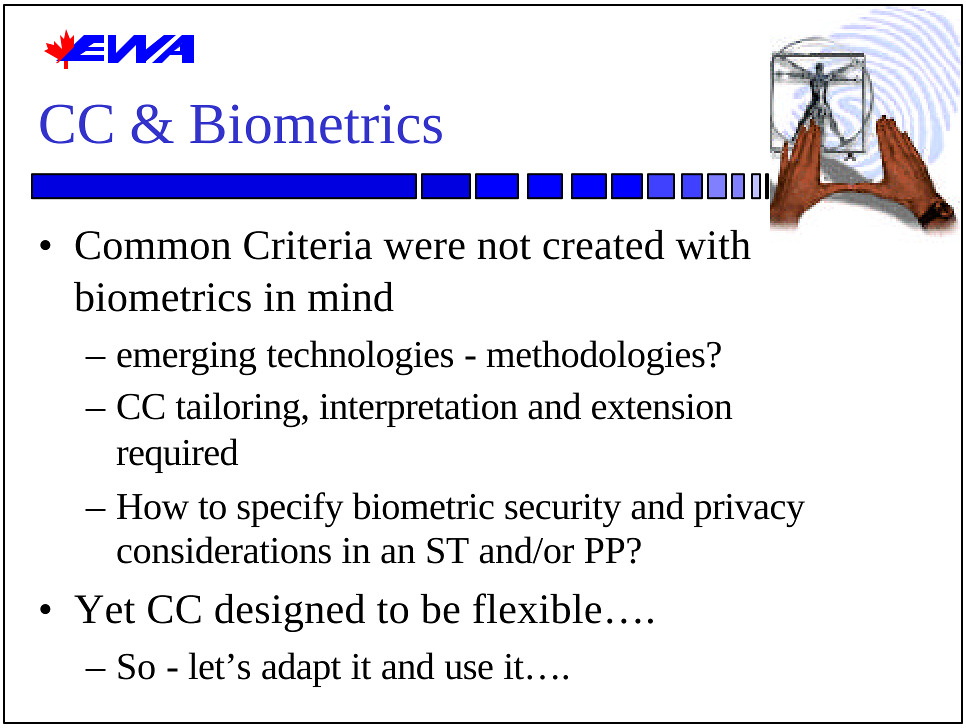
How do the Common Criteria apply to biometrics?



EWA

State of the Practice…..

- Best practices and testing standards for biometrics typically have a “performance” versus “security” focus
- Need:
  - a security-oriented process
    - develop trust and confidence in claims
    - official assurance arguments
  - comprehensive guidance for all aspects of a CC evaluation as applied to biometrics



EWA

CC & Biometrics

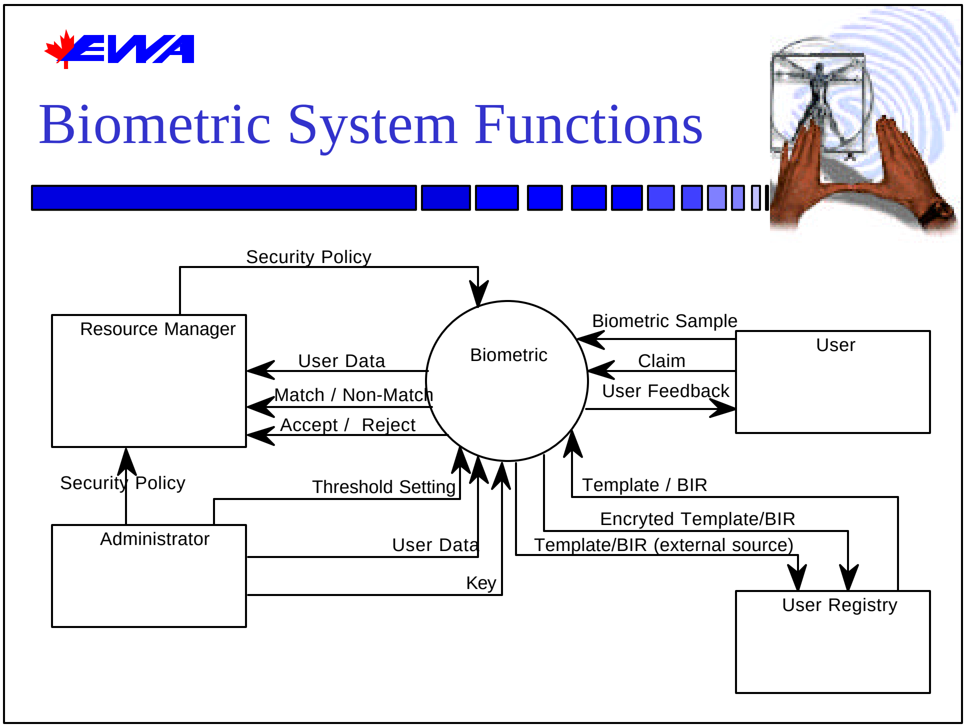
- Common Criteria were not created with biometrics in mind
  - emerging technologies - methodologies?
  - CC tailoring, interpretation and extension required
  - How to specify biometric security and privacy considerations in an ST and/or PP?
- Yet CC designed to be flexible….
  - So - let’s adapt it and use it….

Background Work

- Application of Common Criteria to Biometrics
  - EWA-Canada & Communications Security Establishment jointly conducted a project to consider application of the CC to biometrics
- Context:
  - Bioscrypt Inc. (formerly Mytec Technologies Inc.) sponsored world’s first CC evaluation of a biometric technology

Preparing for Evaluation

- Objective: identify methodology considerations for CC evaluations of biometric technology
- Produced a generic model for biometrics
- Focused in detail on:
  - biometric system functions (versus CC Part 2)
  - security considerations for biometrics
  - security functional and assurance issues
  - test and analysis guidelines



EWA

Biometric System Functions

Security Policy

Resource Manager

Biometric

Biometric Sample

User

User Data

Claim

Match / Non-Match

User Feedback

Accept / Reject

Security Policy

Threshold Setting

Template / BIR

Administrator

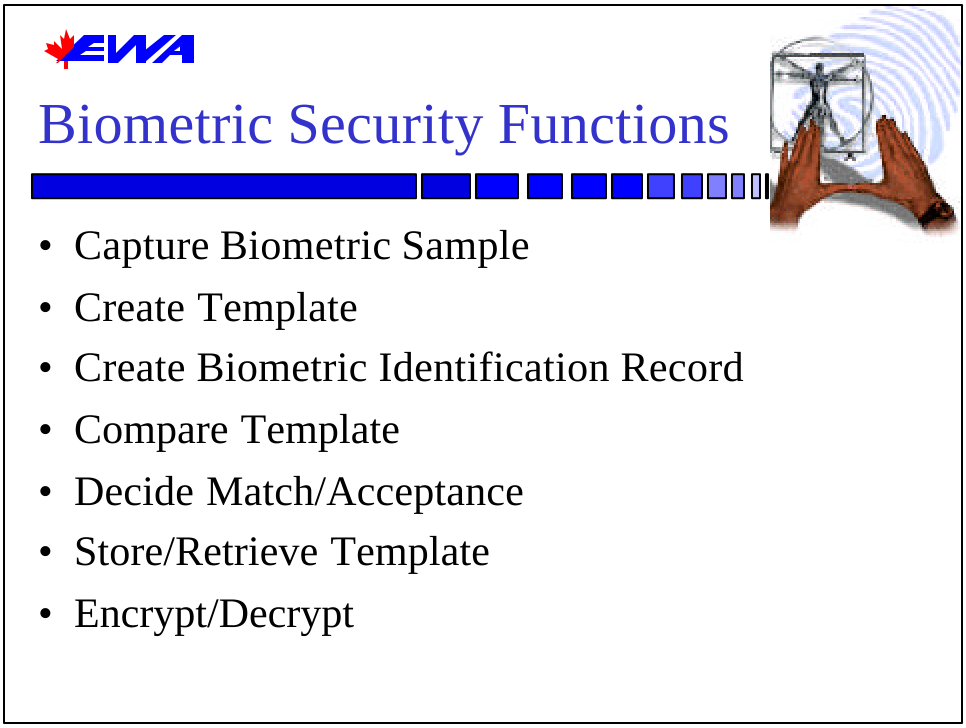
Encryted Template/BIR

User Data

Template/BIR (external source)

Key

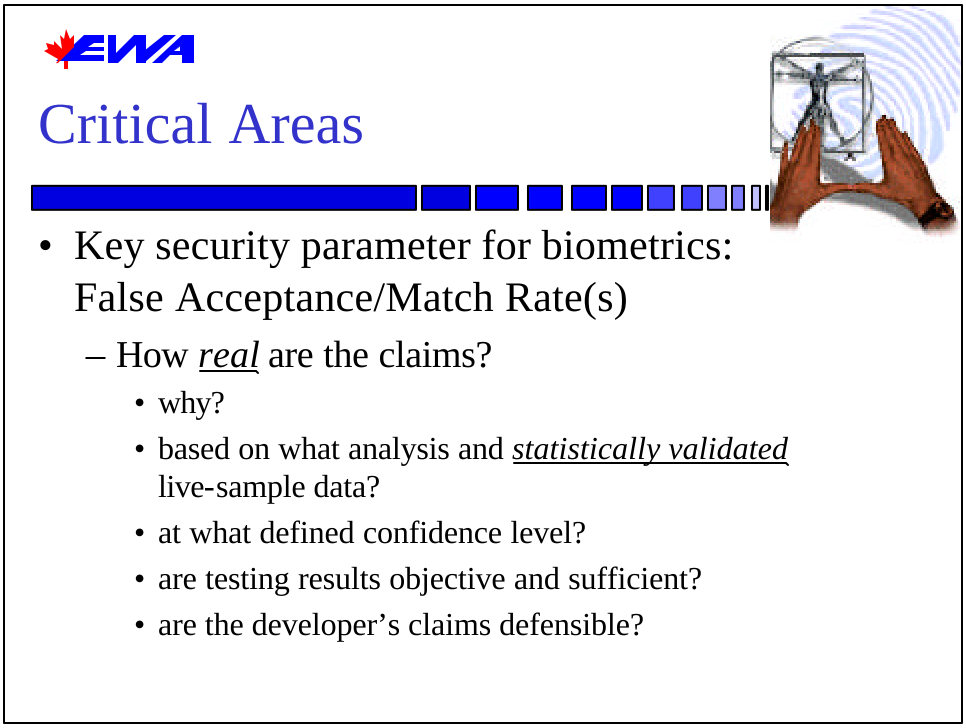
User Registry



EWA

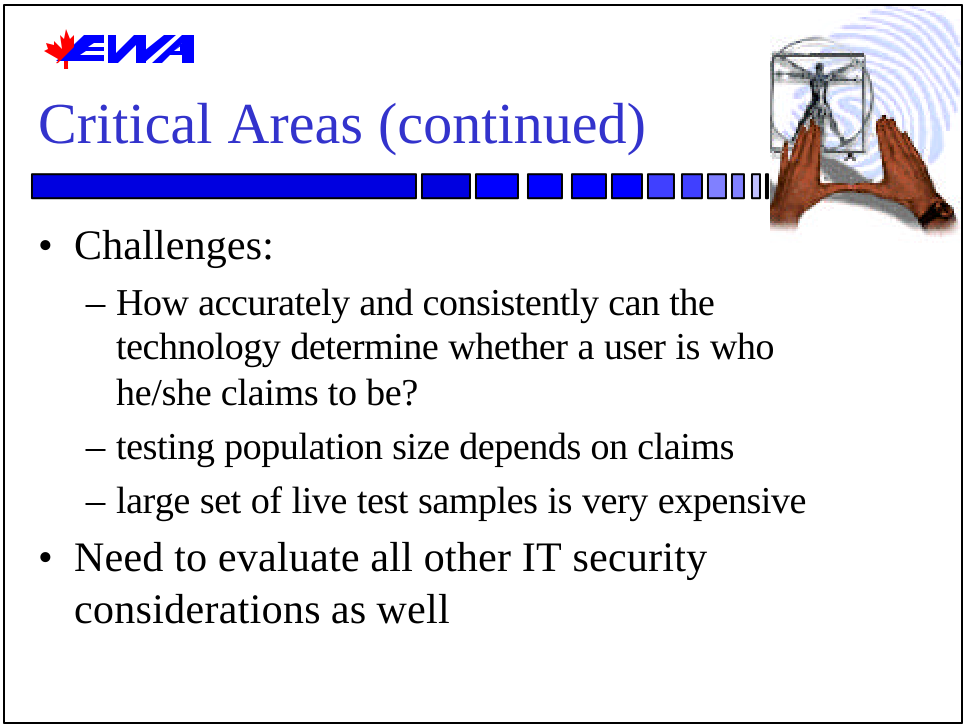
Biometric Security Functions

- Capture Biometric Sample
- Create Template
- Create Biometric Identification Record
- Compare Template
- Decide Match/Acceptance
- Store/Retrieve Template
- Encrypt/Decrypt



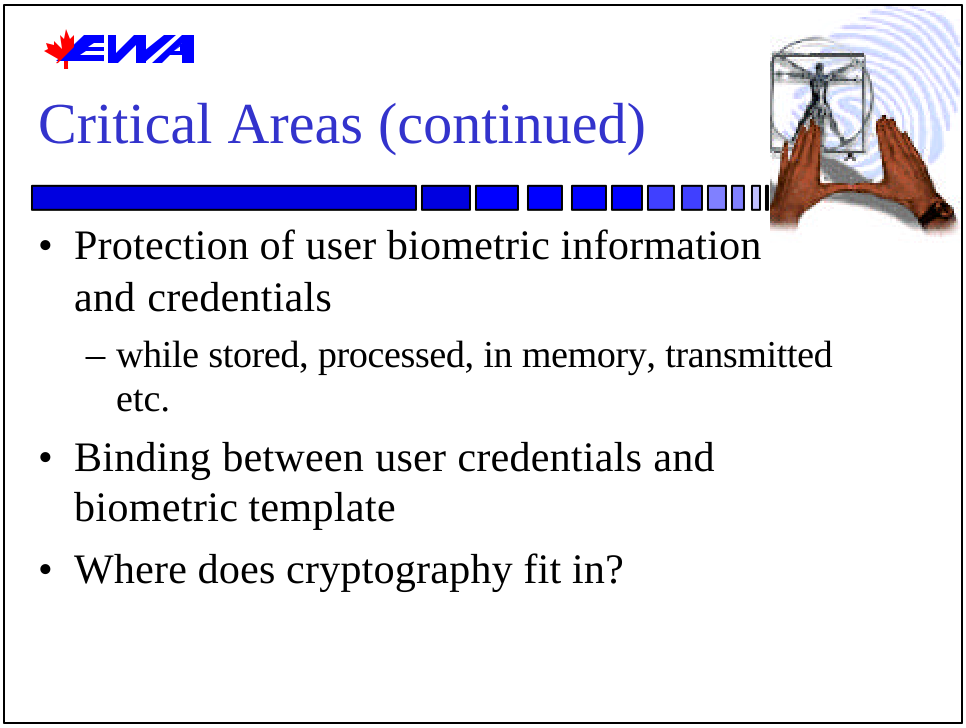
Critical Areas

- Key security parameter for biometrics: False Acceptance/Match Rate(s)
  - How *real* are the claims?
    - why?
    - based on what analysis and *statistically validated* live-sample data?
    - at what defined confidence level?
    - are testing results objective and sufficient?
    - are the developer’s claims defensible?



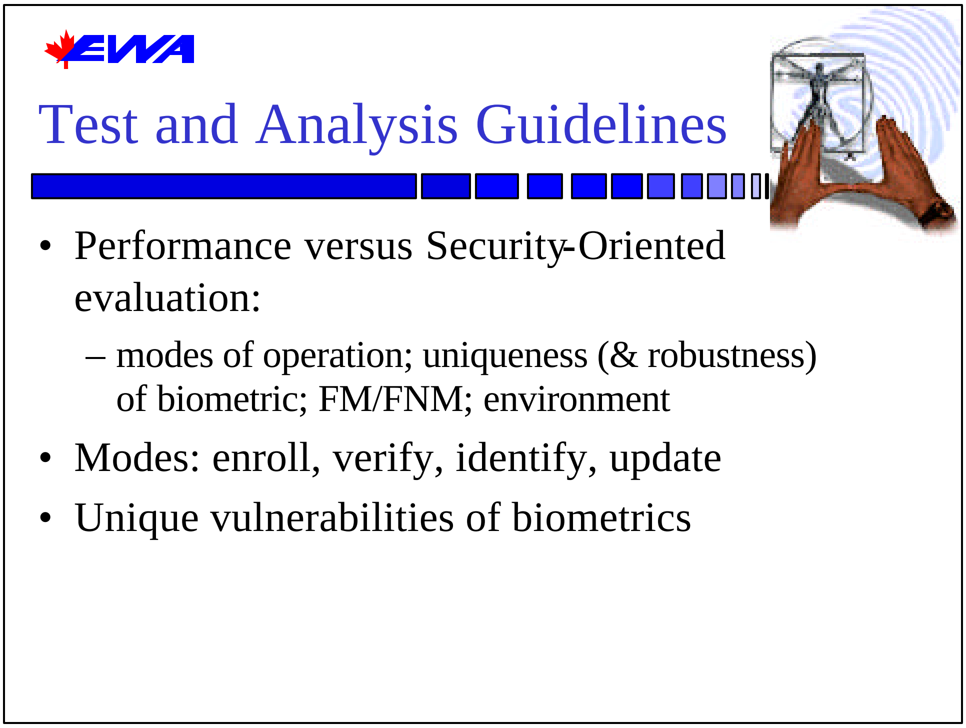
Critical Areas (continued)

- Challenges:
  - How accurately and consistently can the technology determine whether a user is who he/she claims to be?
  - testing population size depends on claims
  - large set of live test samples is very expensive
- Need to evaluate all other IT security considerations as well



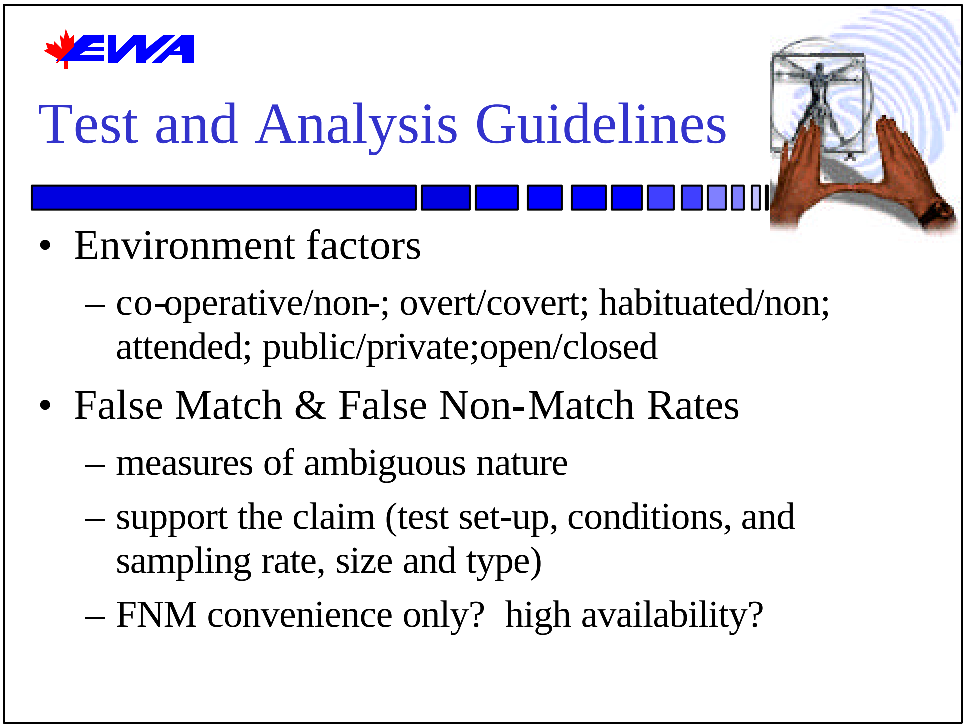
Critical Areas (continued)

- Protection of user biometric information and credentials
  - while stored, processed, in memory, transmitted etc.
- Binding between user credentials and biometric template
- Where does cryptography fit in?



Test and Analysis Guidelines

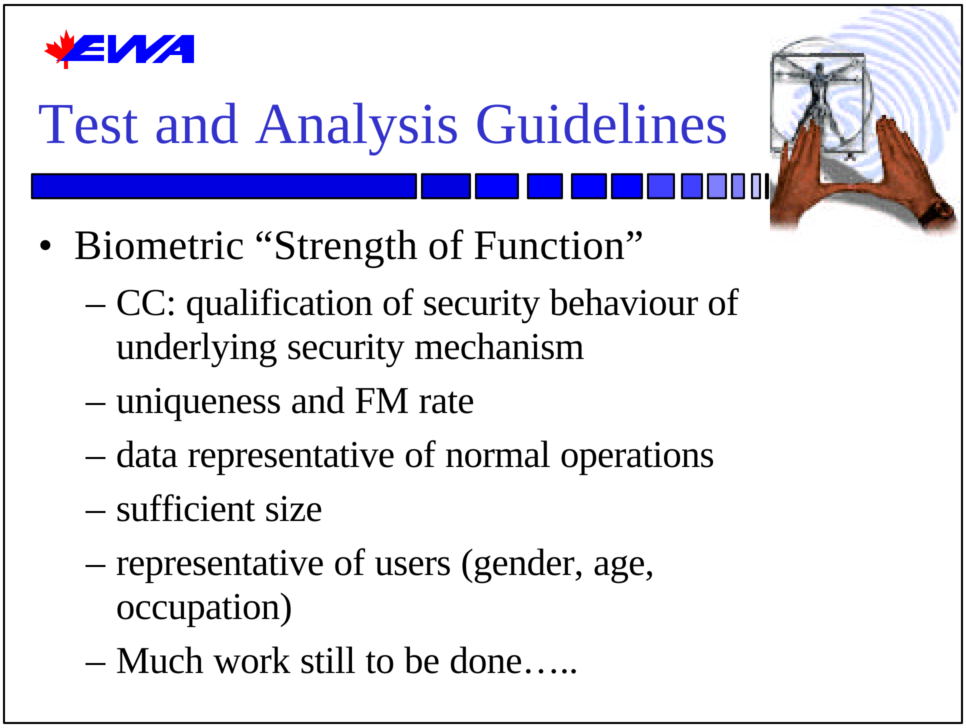
- Performance versus Security-Oriented evaluation:
  - modes of operation; uniqueness (& robustness) of biometric; FM/FNM; environment
- Modes: enroll, verify, identify, update
- Unique vulnerabilities of biometrics



EWA

Test and Analysis Guidelines

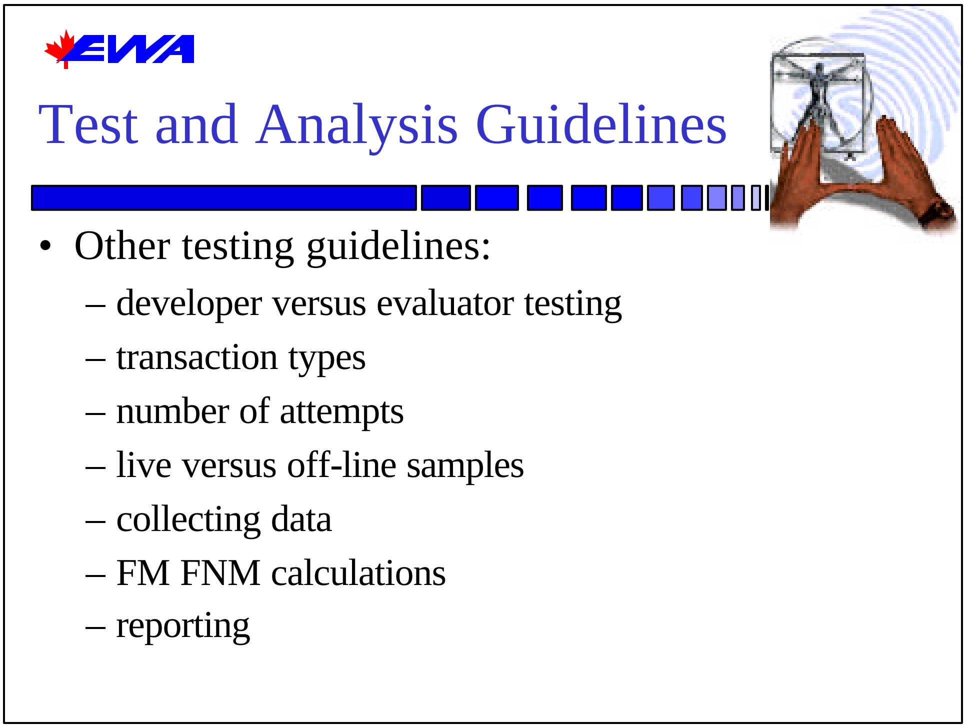
- Environment factors
  - – co-operative/non-; overt/covert; habituated/non; attended; public/private;open/closed
- False Match & False Non-Match Rates
  - – measures of ambiguous nature
  - – support the claim (test set-up, conditions, and sampling rate, size and type)
  - – FNM convenience only? high availability?



EWA

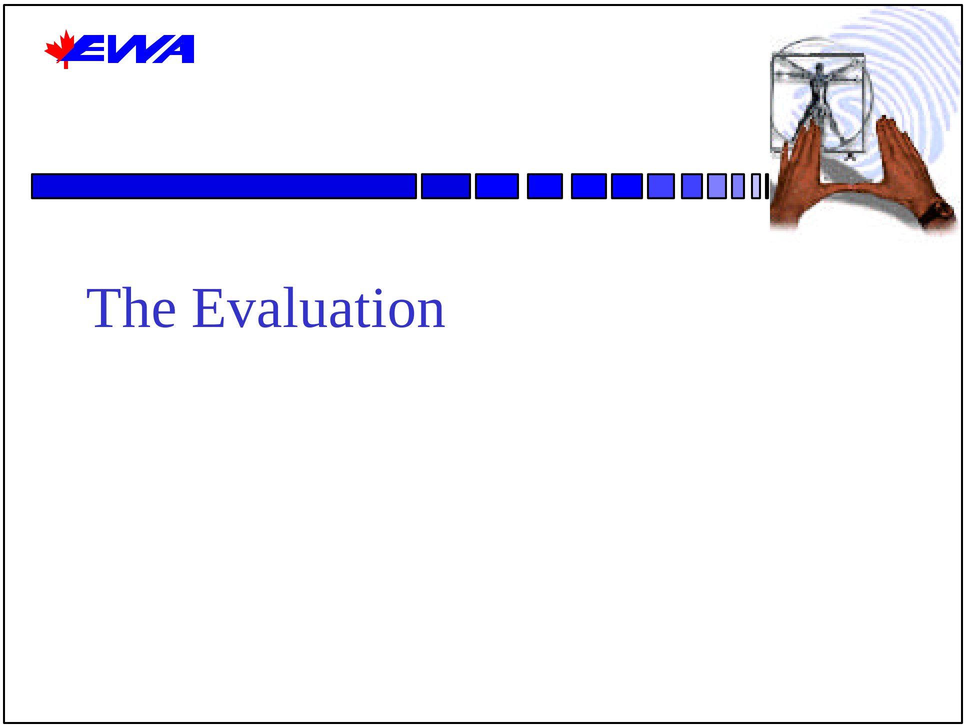
Test and Analysis Guidelines

- Biometric “Strength of Function”
  - – CC: qualification of security behaviour of underlying security mechanism
  - – uniqueness and FM rate
  - – data representative of normal operations
  - – sufficient size
  - – representative of users (gender, age, occupation)
  - – Much work still to be done…..

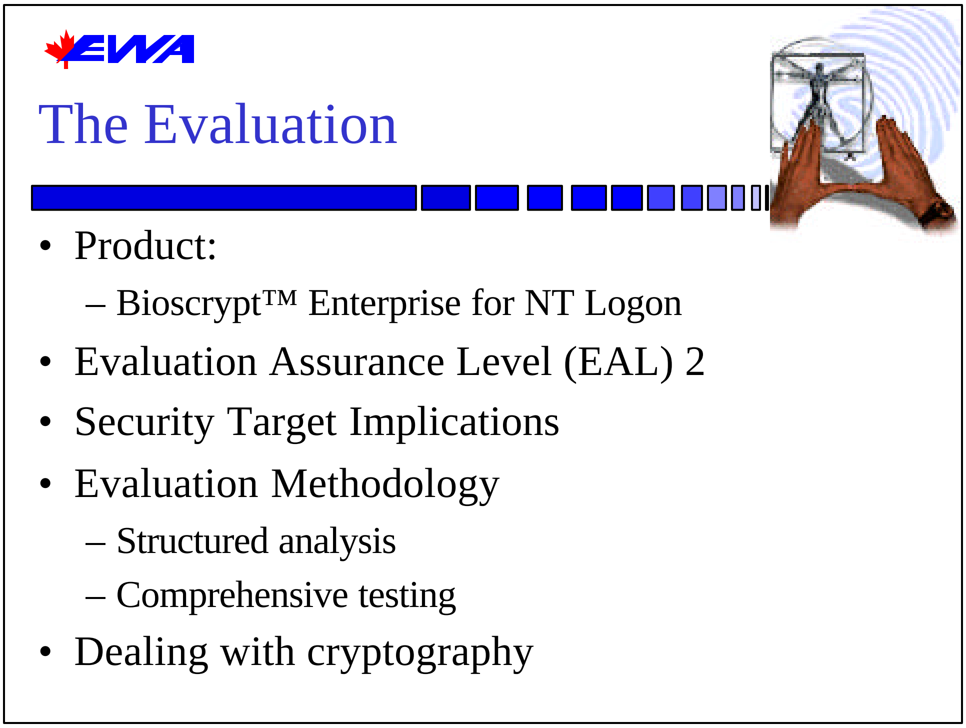


Test and Analysis Guidelines

- Other testing guidelines:
  - – developer versus evaluator testing
  - – transaction types
  - – number of attempts
  - – live versus off-line samples
  - – collecting data
  - – FM FNM calculations
  - – reporting

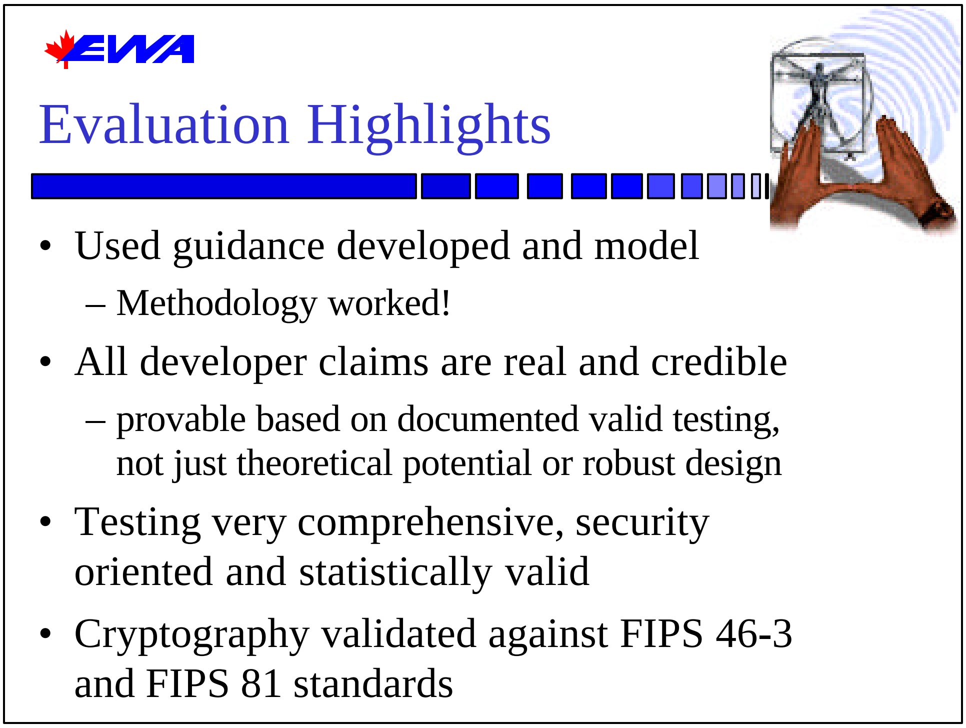


The Evaluation



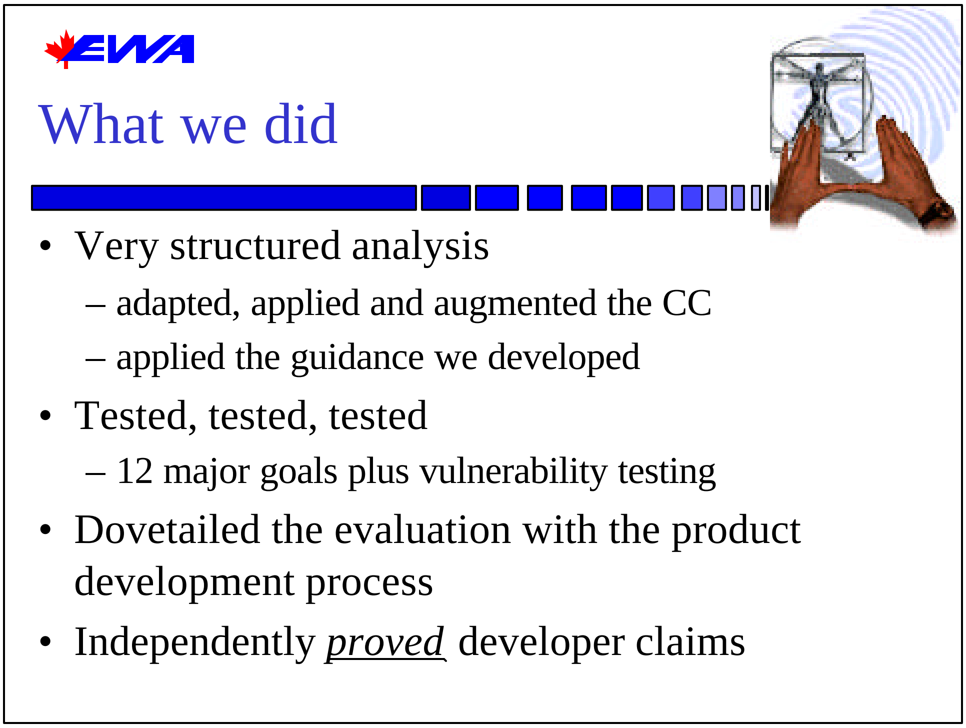
The Evaluation

- Product:
  - Bioscrypt™ Enterprise for NT Logon
- Evaluation Assurance Level (EAL) 2
- Security Target Implications
- Evaluation Methodology
  - Structured analysis
  - Comprehensive testing
- Dealing with cryptography



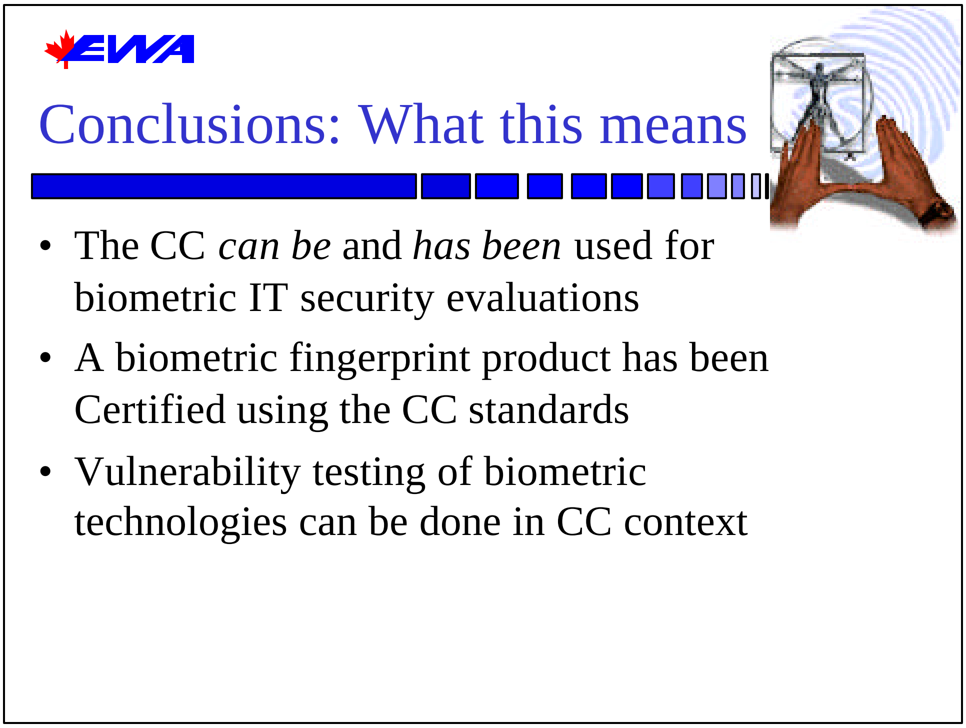
Evaluation Highlights

- Used guidance developed and model
  - Methodology worked!
- All developer claims are real and credible
  - provable based on documented valid testing, not just theoretical potential or robust design
- Testing very comprehensive, security oriented and statistically valid
- Cryptography validated against FIPS 46-3 and FIPS 81 standards



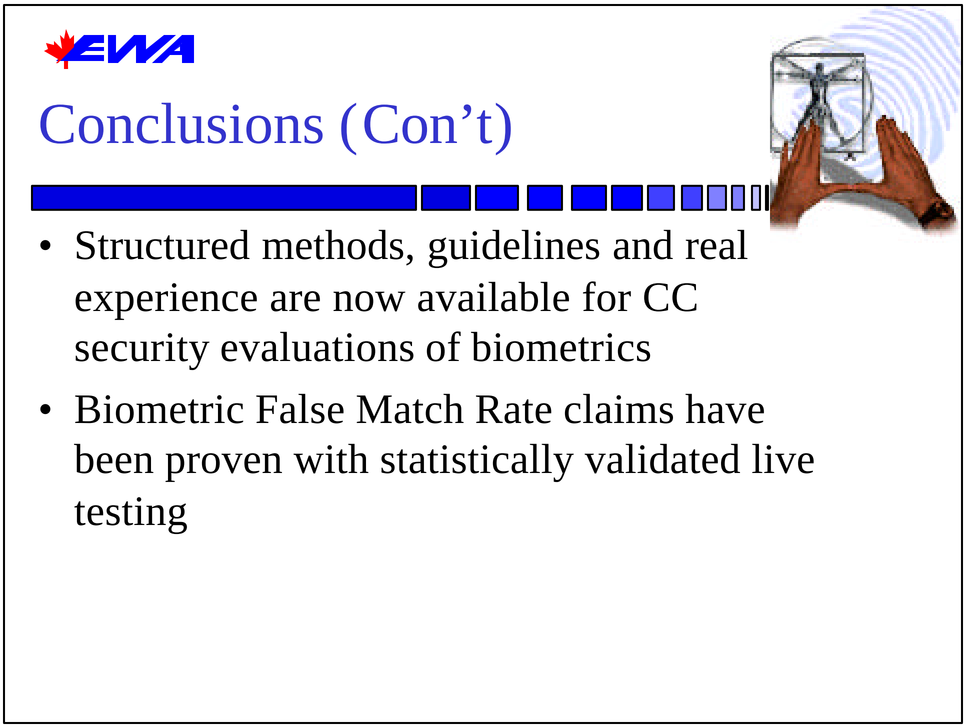
What we did

- Very structured analysis
  - adapted, applied and augmented the CC
  - applied the guidance we developed
- Tested, tested, tested
  - 12 major goals plus vulnerability testing
- Dovetailed the evaluation with the product development process
- Independently *proved* developer claims



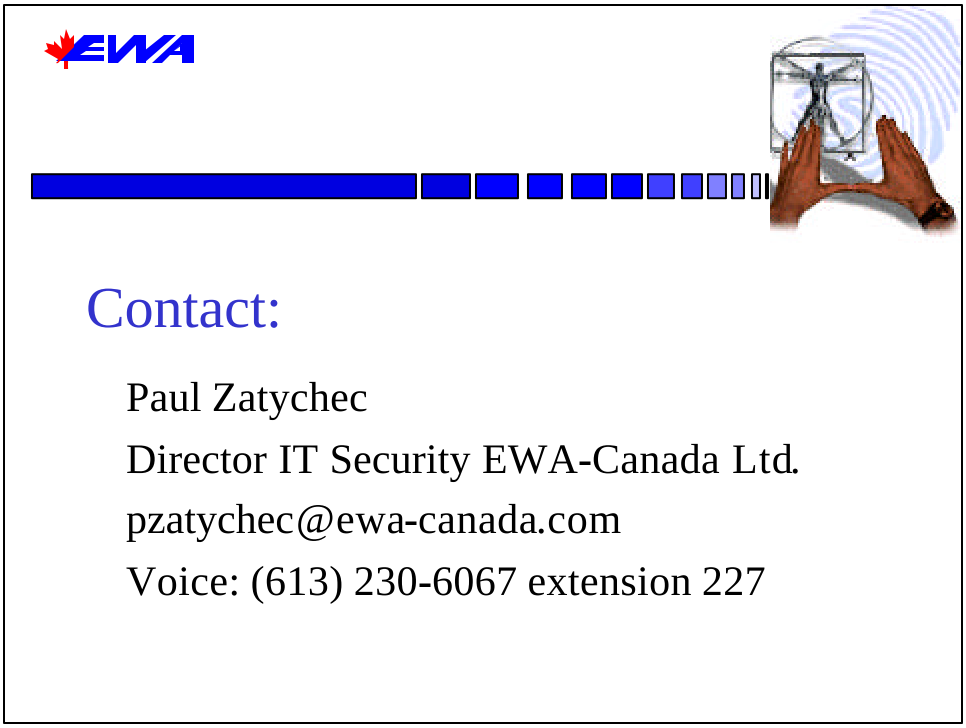
Conclusions: What this means

- The CC *can be* and *has been* used for biometric IT security evaluations
- A biometric fingerprint product has been Certified using the CC standards
- Vulnerability testing of biometric technologies can be done in CC context



Conclusions (Con’t)

- Structured methods, guidelines and real experience are now available for CC security evaluations of biometrics
- Biometric False Match Rate claims have been proven with statistically validated live testing



Contact:

Paul Zatychec
Director IT Security EWA-Canada Ltd.
pzatychec@ewa-canada.com
Voice: (613) 230-6067 extension 227